State of North Carolina

Information Resource Management Commission

Statewide Information Security Assessment Project Summary Report Agency Name

Version No. Draft 1

November 14, 2003

Table of Contents

Executive Summary

Purpose

In accordance with Section 1 (a) G.S. 147-33.82 of North Carolina Session Law 2003-153, which requires that “the State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards” on a yearly basis, an assessment of the information security posture of the Agency Name was conducted during October and November of 2003. The information security assessment was conducted by Vendor Name as directed by the State Chief Information Officer. Project operations were managed by the State Chief Information Security Officer through the State Information Security Office’s Project Management Office.

To ensure uniformity of process and consistency of results, the assessment was conducted using tools and templates developed by the Project Management Office based upon the statewide blended security framework including federal and state legislative requirements and the ISO 17799 information security standard.

The assessment process is ultimately intended to provide State decision makers with: 1) a global view of the security status of agencies, and, 2) specific assessment findings in detail sufficient to permit the State to prioritize and budget for required security enhancement efforts. This document and its attachments report the results of the security assessment for the Agency Name.

Agency Mission and Unique Responsibilities

The primary mission of the Agency Name is to [Instructions: include the agency’s mission statement, list of services provided, business functions, etc.]. The unique security requirements associated with the agencies special business requirements include:

- [Instructions: include all special information security needs (e.g. confidentiality, integrity, and availability) (i.e. protect criminal records) and corresponding security compliance requirements (i.e. HIPAA, NCIC, FERPA, etc.)]
-

Summary of Major Findings

The following discussion provides an overview of major assessment findings and related analysis. Additional supporting detail regarding salient findings can be found in the following section. A complete catalog of findings, captured in the assessment tool, can be found in Appendix A.

Agency Best Practices

[Instructions: Provide a paragraph(s) that describe(s) the strengths of the agency's overall security posture. The focus of this section should be at the category level ("Physical security is an agency strength…"). Illustrate using specific examples of agency PSP or deployment that conform to best practice (i.e. – score of "1"). If the agency does not have any significant current security strengths, please include details on several in-progress projects that are expected to result in strengths.]

Agency Opportunities for Improvement

[Provide a paragraph(s) that describe(s) the limitations of the agency's overall security posture. The focus of this section should be at the category level. Illustrate using specific examples of agency PSP or deployment that represent significant risks to the business (i.e. score of "4" or "3" with "High" or "Medium" risk. Although the number of findings listed here may vary from agency to agency, think in terms of "top five" of the eleven categories for improvement.]

Overall Score and Score Interpretation

In order to provide an accurate and multi-dimensional view of the agency's information security posture, the assessment tool required that the agency be quantitatively scored against two scoring categories – "Quality" and "Execution". Scoring was administered on a graduated scale where a score or "1" represents the highest or best possible mark, and a score of "4" represents the lowest or worst possible mark.

Quality Score

Overall Quality Score: X.X
The Quality score represents whether the agency has addressed its information security requirements in an effective and complete fashion in its Policies, Standards and Procedures (PSP). Quality scores are as follows:

- "1" indicates that the agency's Policies, Standards and Procedures conform to best practices
- "2" indicates that PSP meet requirements
- "3" indicates that the PSP are deficient
- "4" indicates that the agency's PSP do not meet requirements.

Execution Score

Overall Execution Score: X.X
The Execution score represents whether the agency has deployed information security Policies, Standards and Procedures in an encompassing fashion. Execution scores are as follows:

- "1" indicates that PSP are fully or universally deployed
- "2" indicates that PSP are deployed for critical areas only

- “3” indicates that there are gaps in deployment
- “4” indicates that the there are no PSP in-effect or deployed, or that agency PSP are still in development.

Agency Security Posture Dashboard

The following diagrams pictorially depict the overall status of the agency’s security posture.

[Diagrams and additional explanation of diagram content will be added by the PMO at a future date.]

Recommended Remediation Priorities

Based upon the assessment findings, the following corrective actions are recommended by the assessment team to improve the agency’s information security posture.

[Instructions: Define the top 3 – 5 priorities for remediation activities with a short description of the issue, the recommended correction actions, and the benefits accruing from the corrective action. These remediation recommendations are intended to focus on high-level, high-priority needs that would resolve one or more critical findings. List recommendations in highest-to-lowest order of priority.]

Recommendation One

Findings Summary	
Corrective Action	
Benefit	

Recommendation Two

Findings Summary	
Corrective Action	
Benefit	

Recommendation Three

Findings Summary	
Corrective Action	
Benefit	

Findings, Analysis, and Recommendations

The following discussion identifies additional findings and risks, provides additional detail regarding those risks and provides high-level recommendations for corrective action. Findings are grouped in correspondence with the state information security and assessment tool frameworks.

1. Security Policies, Standards and Procedures (PSP)

Quality Score: X.X; Execution Score: X.X

Security Policies, Standards and Procedures control addresses management support, commitment, and direction in accomplishing information security goals. Key findings related to Security Policy include:

[Instructions: Identify several best practices and the top areas for improvement. The intent is cogently document critical findings. Most agencies will have at least two findings per section; some as many as seven or eight. Remember of express findings in lay terms, and avoid including any information that might further compromise the agency's security posture.]

1. Best Practice: (Tool ID Number) (i.e. – (1.2.5)) – Findings description. [Include salient findings with a score of 1. Where possible, combine specific findings into a more generalized statement. Example – "Best Practice: (1.1.1 – 1.1.12) Agency policies are complete, up-to-date, and conform with industry best practices"]

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action. [Include notable findings with a score of 4 or major findings with a score of 3.]

3. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

4. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

2. Organizational Security

Quality Score: X.X; Execution Score: X.X

Organizational Security control addresses the need for a management framework that creates, sustains, and manages the security infrastructure. Key findings related to Organizational Security Policy include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

3. Asset Classification and Control

Quality Score: X.X; Execution Score: X.X
Asset Classification and Control addresses the ability of the security infrastructure to protect organizational assets. Key findings related to Asset Classification and Control include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

4. Personnel Security

Quality Score: X.X; Execution Score: X.X
Personnel Security control addresses an organization's ability to mitigate risk inherent in human interactions. Key findings related to Personnel Security include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

5. Physical Security

Quality Score: X.X; Execution Score: X.X
Physical Security control addresses risk inherent to organizational premises. Key findings related to Physical and Environmental Security include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

6. Communications and Operations Management

Quality Score: X.X; Execution Score: X.X
Communication and Operations Management control addresses an organization's ability to ensure correct and secure operation of its assets. Key findings related to Communications and Operations Management include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

7A. Access Administration

Quality Score: X.X; Execution Score: X.X

Access Administration control addresses the administrative aspects of an organization's ability to control access to assets based on business and security requirements. Key findings related to Access Administration Control include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

7B. Access Technology

Quality Score: X.X; Execution Score: X.X

Access Technology control addresses the technological aspects of an organization's ability to control access to assets based on business and security requirements. Key findings related to Access Technology Control include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

8. Applications Development and Maintenance

Quality Score: X.X; Execution Score: X.X

Applications Development and Maintenance control addresses an organization's ability to ensure that appropriate information system applications security controls are both incorporated and maintained. Key findings related to Applications Development and Maintenance include:

1. Best Practice: (Tool ID Number) – Findings description.

2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

9. Business Impact/Continuity Management

Quality Score: X.X; Execution Score: X.X
Business Impact/Continuity Management control addresses an organization's ability to counteract interruptions to normal operations. Key findings related to Business Impact/Continuity Management include:

1. Best Practice: (Tool ID Number) – Findings description.
2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

10. Compliance

Quality Score: X.X; Execution Score: X.X
Compliance control addresses an organization's ability to remain in compliance with regulatory, statutory, contractual, and security requirements. Key findings related to Compliance include:

1. Best Practice: (Tool ID Number) – Findings description.
2. Opportunity for Improvement: (Tool ID Number) – Findings description. Description of potential business impact. Description of recommended corrective action.

Appendices

A. Agency Security Assessment Tool

B. Agency Response to Security Assessment Findings